below line 16, insert

-- The above-described method and communication system are illustrative of the principles of the present invention. Numerous modifications and adaptions thereof will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.--.

IN THE CLAIMS:

On page 12, line 1, replace "**PATENT CLAIMS**" with --WHAT IS CLAIMED IS:--

Please amend claims 1-15 as follows:

1. (Amended) A method [Method] for encryption of information for a radio transmission and for authentication of subscribers [(S1, S2)] in a communication system [(UNM),] that [-] comprises an access network [(ACN)] having equipment [(BS, BSC)] for said [the] radio transmission, said communication system further comprising a [as well as at least one] core network [(CON1, CON2)] having a respective authentication equipment [(AC, AC=)] for said [the] subscriber authentication, comprising the steps of:

[- allocates] allocating a radio channel [(RCH)] for said [the] transmission of said [the] information via a radio interface [(AI)] from/to a [at least one] base station [(BS)] of said [the] access network; [(ACN), whereby]

[-] mutually transmitting public keys [(PUK1-MT, PUK-BS) are mutually transmitted] between a mobile station [(MT)] and said [the] base station [(BS)] via said [the] radio interface; [(AI),]

[-] encrypting subsequent information to be transmitted via said radio interface using one of said [the] public keys [key (PUK1-MT or, respectively, PUK-BS)] received by said [the] base station [(BS)] or [, respectively,] said mobile station; [(MT) is employed for encryption of the information to be subsequently transmitted via the radio interface (AI),]

[- the] deciphering encrypted information received by said [the] mobile station [(MT)] or [, respectively,] said base station [(BS) are deciphered] on the basis of a private key [(PRK1-MT, PRK1-BS)] that is allocated to said [the] transmitted, public key [(PUK1-MT, PUK-BS)] in said [the] mobile station [(MT)] or [, respectively,] in said [the] base station; and [(BS), and whereby]

[-] authenticating said core network via a subscriber identity mobile card [-specific means (SIN)] of said [the] mobile station [(MT) implements the authentication of the respective core network (CON1, CON2)], and authenticating said subscribers via said authentication equipment [the means (AC, AC=)] of said [the] core network [(CON1, CON2) implements the authentication of the subscriber (S1, S2)] on the basis of encrypted information that have been mutually sent.

2. (Amended) A method [Method] according to claim 1, further comprising the steps of: [whereby]

[-] sending a first public key [(PUK1-MT) is first sent] from said [the] mobile station [(MT)] to said [the] base station; [(BS),]

encrypting [which employs it for the encryption of the] information to be sent to said [by the] mobile station [(MT)] using said first public key by said base station;

[- a] sending an other public key [(PUK-BS) is sent] from said [the] base station [(BS)] to said [the] mobile station; [(MT),]

encrypting [which employs it for the encryption of the] information to be sent to said [the] base station [(BS)] using said other public key by said mobile station, and; [and, subsequently,]

[- the mobile station (MT) sends] sending a second public key [(PUK2-MT)] to said [the] base station [(BS)] by said mobile station subsequent to said step of sending said other public key from said base station.

3. (Amended) A method [Method] according to claim 2, further comprising the step of replacing said first [whereby the second] public key [(PUK2-MT) replaces the first] with said second public key [(PUK1-MT)] sent to said [the] base station [(BS)].

4. (Amended) A method [Method] according to claim 1, further comprising the steps of: [whereby

- the base station (BS) first sends a first public key (PUK1-BS) to the mobile station (MT) that employs for encryption of the information to be sent to the base station (BS);

- the mobile station (MT) sends a public key (PUK-MT) to the base station (BS) that employs for the encryption of the information to be sent to the mobile station (MT); and, subsequently,

- the base station (BS) sends a second public key (PUK2-BS) to the mobile station (MT).]

sending a first public key from said base station to said mobile system;

encrypting information to be sent to said base station using said first public key by said mobile station;

sending an other public key from said mobile station to said base station;

encrypting information to be sent to said mobile station using said other public key by said mobile station; and

sending a second public key to said mobile station by said base station subsequent to said step of sending said other public key from said mobile station.

5. (Amended) A method [Method] according to claim 4, further comprising the step of replacing said first [whereby the second] public key [(PUK2-BS) replaces the first] with said second public key [(PUK1-BS)] sent to said [the] base station [(BS)].

6. (Amended) A method [Method] according to claim 1, further comprising the steps of: [one of the preceding claims, whereby]

[- the mobile station (MT) sends] sending a subscriber identity [(SID)] of said [the] subscriber [(S1, S2)] and an authentication request [(aureq-mt)] by said mobile station to said [the] core network [(CON1, CON2)] in encrypted form; [, and]

returning, by said authenticating equipment [the means (AC, AC=)] of the core network, [(CON1, CON2) returns] an authentication reply [(aures-co)] in encrypted form; and

[- the] implementing, by said mobile station, [(MT) implements] an authentication procedure for checking an [the] identity of said [the] core network [(CON1, CON2)].

7. (Amended) A method [Method] according to claim 6, further comprising the steps of: [whereby]

[- the means (AC, AC=) of the core network (CON1, CON2) sends] sending an authentication request [(aureq-co)] in addition to said [the] authentication reply (aures-co) in encrypted form by said authenticating equipment of said core network; [, and]

returning, by said [the] mobile station, [(MT) returns] an authentication reply [(aures-mt)] to said authenticating equipment of said core network [the means (AC)] in encrypted form; and

[- the means (AC, AC=) implements] checking said subscriber identity by an authentication procedure implemented by said authenticating equipment of said core network [for checking the subscriber identity (SID)].

8. (Amended) A method [Method] according to claim 1, further comprising the step of implementing said authentication procedure utilizing [one of the preceding claims, whereby] secret keys [(ki) are employed for the authentication procedure].

9. (Amended) A method [Method] according to claim 1, further comprising the steps of: [one of the preceding claims, whereby]

servicing, by said [the] access network [(ACN) services] at least two core networks [(CON1, CON2)] in parallel; and

registering and authenticating in different core networks, a subscriber [one or more subscribers (S1, S2)] that can use said [the] mobile station [(MT)] in parallel [are registered and authenticated in different core networks (CON1, CON2)].

10. (Amended) A method [Method] according to claim 1, further comprising the step of: [one of the claims 1 through 8, whereby the]

servicing, by access network, [(ACN) services] a core network [(CON)] in which a plurality of subscribers [(S1, S2)] that can use said [the] mobile station [(MT)] in parallel are registered and authenticated.

11. (Amended) A method [Method] according to claim 1, wherein said [one of the preceding claims, whereby the] access network [(ACN)] and said [the] core network or multiple core networks [(CON1, CON2)] are administered by different network operators.

12. (Amended) A communication [Communication] system for encryption of information for a radio transmission and for authentication of subscribers [(S1, S2)], comprising:

[-] an access network [(ACN)] having equipment [(BS, BSC)] for said [the] radio transmission as well as a [at least one] core network [(CON1, CON2)], said core network having a respective authentication equipment [means (AC, AC=)] for said [the] subscriber authentication, said communication system utilizing

[-] a radio channel [(RCH)] for transmission of said information [the intervention] via a radio interface [(AI)] from/to a [at least one] base station [(BS)] of the access network; [(ACN),

and comprising]

[-] memory devices [(MSP, BSP)] in a mobile station [(MT)] and in said [the] base station [(BS)] for storing public keys [(PUK1-MT, PUK-BS)] and private keys [PRK1-BS, PRK1-BS [sic])] that are allocated to said [the] public keys [(PUK1-MT, PUK-BS)],

[- transmission devices (MSE, BSE)] transmitters in said [the] mobile station [(MT)] and in said [the] base station [(BS)] for mutually sending said [the] public keys [(PUK1-MT, PUK1-BS)] via said [the] radio interface; [(AI),]

[- control devices (MST, BST)] controllers in said [the] mobile station [(MT)] and in said [the] base station [(BS)] for encryption of said [the] information to be subsequently sent via said [the] radio interface [(A1)] upon employment of said [the] public keys [(PUK1-MT or, respectively, PUK-BS)] received by said [the] base station [(BS)] or, respectively, said mobile station [(MT)] and for deciphering [the] received, encrypted information on the basis of said [the] stored, appertaining private key [(PRK1-MT, PRK1-BS), and]

said mobile station comprising [-] a subscriber identity mobile card [-specific means (SIN) in the mobile station (MT) and a means (AC, AC=) in the respective core network (CON1, CON2)] for authenticating said [the implementation of the authentication of the] core network; [(CON1, CON2) as well as]

said core network comprising an authentication equipment for authenticating said [the authentication of the] subscribers; and [(S1, S2)]

said authenticating said core network and said authenticating said subscribers utilizing [on the basis of] mutually transmitted, encrypted information.

13. (Amended) A communication [Communication] system according to claim 12, wherein said [comprising an] access network [(ACN) to which] has at least two core networks [(CON1, CON2) are] connected in parallel for [the] registration and authentication of a subscriber [one or more subscribers (S1, S2)] that can use said [the] mobile station [(MT)] in parallel in different core network

[(CON1, CON2)].

14. (Amended) A communication [Communication] system according to claim 12, wherein said [comprising an] access network [(ACN) to which] has a core network [(CON1) is] connected for [the] registration and authentication of a plurality of subscribers [(S1, S2)] that can use said [the] mobile station [(MT)] in parallel.

AF cont'd.

15. (Amended) A communication [Communication] system according to claim 12 [one of the preceding claims, comprising an] wherein said access network [(ACN)] and said core network or multiple core networks are administered by [one or more core networks (CON1, CON2) that exhibit] different network operators.

IN THE ABSTRACT

On page 17:

cancel lines 2-3;

in line 9, cancel ", respectively,";

in line 10, cancel ", respectively,";

in line 13, cancel ", respectively,";

in line 15, cancel ", respectively,";

in line 16, cancel "mobile radio telephone-specific means (SIN)" and substitute --subscriber identity mobile card (SIM)-- therefor;

in line 18, cancel "a means" and substitute --authentication equipment-- therefor; and

cancel line 21.